PATENT
Docket No. **VIV/0012.01**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Steven L. Teixeira	Examiner: Lashley, Laurel L
Serial No.: 10/605,644	Art Unit: 2132
Filed: October 15, 2003	APPEAL BRIEF
For: System and Methodology Providing Information Lockbox	

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON BEHALF OF STEVEN L. TEIXEIRA

This is an appeal from the Final Rejection mailed 06/11/2007, in which currently-pending claims 1-55 stand finally rejected. Appellant filed a Notice of Appeal on 09-13-2007. This brief is submitted electronically in support of Appellant's appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Check Point Software Technologies, Inc. located at 800 Bridge Parkway, Redwood City, CA 94065.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellant, the Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

The status of all claims in the proceeding is as follows:

Rejected: Claims 1-55

Allowed or Confirmed: None

Withdrawn: None

Objected to: None

Canceled: None

Identification of claims that are being appealed: Claims 1-55

An appendix setting forth the claims involved in the appeal is included as the last section of this brief.

4. STATUS OF AMENDMENTS

One Amendment has been filed in this case. Appellant filed an Amendment on 03/12/2007, in response to a non-final Office Action dated 12/12/2006. In the Amendment, the pending claims were amended in a manner which Appellant believes clearly distinguished the claimed invention over the art of record, for overcoming the art rejections. In response to the Examiner's Final Rejection dated 06/11/2007, Appellant filed a Notice of Appeal. Appellant has chosen to forgo filing an Amendment After Final which might further limit Appellant's claims, as it is believed that further amendments to the claims are not warranted in view of the art. Accordingly, no Amendments have been entered in this case after the date of the Final Rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

A. First (and single) Ground

As to Appellant's First Ground for appeal, Appellant asserts that the art rejection relying on Margolus et al. fails to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 1**: in a computer system, a method for protecting sensitive information (see, e.g., Appellant's specification at Fig. 5 and paragraphs [0062-0063]), the method comprises steps of: receiving input of sensitive information from a user (see, e.g., Appellant's specification at Fig. 5 at step 501, and paragraph [0063]); computing a data shadow of the sensitive information for storage in a repository and thereafter discarding the input so that the sensitive information itself is not stored (see, e.g., Appellant's specification at Fig. 5 at step 502, and paragraph [0063]; see also paragraph [0078] for discussion about how the underlying input data itself is not stored); based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information (see, e.g., Appellant's specification at Fig. 5 at step 503, and paragraph [0063]); and blocking any detected attempt to transmit the sensitive information that is not authorized by the user (see, e.g., Appellant's specification at Fig. 5 at step 504, and paragraph [0063]).

Appellant further asserts that the art rejection relying on Margolus et al. fails to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 33**: in a computer system, a method of the present invention is described for securing sensitive items from inappropriate access (see, e.g., Appellant's specification at Fig. 5 and paragraphs [0062-0063]), the method comprises steps of: receiving input from a user indicating that a particular sensitive item is to be protected from inappropriate access (see, e.g., Appellant's specification at Fig. 5 at step 501, and paragraph [0063]); storing metadata characterizing the particular sensitive item, and thereafter discarding the input so that the particular sensitive item itself is not stored (see, e.g., Appellant's specification at Fig. 5 at step 502, and paragraph [0063]; see also paragraph [0078] for discussion about how the underlying input data itself is not stored); based on the stored metadata, detecting whether the particular sensitive item is present in any transmission of outgoing

data (see, e.g., Appellant's specification at Fig. 5 at step 503, and paragraph [0063]); and trapping any transmission of outgoing data that is detected to contain the particular sensitive item (see, e.g., Appellant's specification at Fig. 5 at step 504, and paragraph [0063]).

Appellant further asserts that the art rejection relying on Margolus et al. fails to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 47**: a system of the present invention providing security for sensitive information that comprises: a data processing system (see, e.g., Appellant's specification at system 100 (Fig. 1)) receiving input of sensitive information (see, e.g., Appellant's specification at Fig. 5 at step 501, and paragraph [0063]); a secure lockbox module for storing a secure descriptor characterizing the sensitive information, so that the system can detect transmission of the sensitive information without a copy of the sensitive information itself being stored (see, e.g., Appellant's specification at lockbox subsystem 401, Fig. 4, and paragraphs [0058-0059]); and a security module for detecting, based on the secure descriptor, any attempted transmission of outgoing data that contains the sensitive information (see, e.g., Appellant's specification at Fig. 5 at step 503, and paragraph [0063]; see also security/rules (TrueVector) engine 441, Fig. 4, which is in communication with lockbox subsystem 401, and description at paragraphs [0057-0061]).

6. GROUNDS OF REJECTION TO BE REVIEWED

The grounds presented on appeal are:

(1st) Whether claims 1-55 are unpatentable under 35 U.S.C. Section 102(e) as being anticipated by Margolus et al. US Patent Publication No. 2004/0162808 (hereinafter, "Margolus").

7. ARGUMENT

A. First (and single) Ground: Claims 1-55 rejected under Section 102(e)

1. General

Under Section 102, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, the reference fails

to teach each and every element set forth in Appellant's independent claims, as well as other claims, and therefore fails to establish anticipation of the claimed invention under Section 102.

2. Claims 1-55: Margolus

Claims 1-55 stand rejected under 35 U.S.C. 102(e) as being anticipated by Margolus et al. in US Patent Application Publication No. 2004/0162808 (hereinafter, "Margolus"). Here, the Examiner likens Appellant's invention to Margolus' data repository that promotes network storage of data.

At the outset, it is important to understand that Appellant does not claim to have invented the notion of computing a fingerprint on data. For example, as Margolus aptly points out (e.g., Margolus at [0006]), the concept of a "digital fingerprint" of a file, also called a "hash function", a "content signature" or a "message digest", is well known. Margolus explains, at [0007], that fingerprints have been used for many years to avoid unnecessary file transfers. One application of this sort has been in Bulletin Board Systems (BBSs), which have used fingerprints since the early 1990's to avoid the communication cost of uploading file data that is already present in the BBS, but associated with a different file name. A client computer wishing to upload or store data on the BBS can compute the fingerprint of the file that it wishes to send, and send that first. If a file containing this data is already present in the BBS, then the client is informed and need not send anything. The scheme uses fingerprints to identify redundant data and avoid unnecessary transmission and storage.

With the above basic notion of a digital fingerprint, Margolus describes an approach for promoting network storage of data. Margolus describes a method by which more than one client program connected to a network stores the same data item on a storage device of a data repository connected to the network. The method comprises encrypting the data item using a key derived from the content of the data item, determining a digital fingerprint of the data item, and **storing the data item on the storage device** at a location or locations associated with the digital fingerprint. Importantly, as indicated by the foregoing highlights, Margolus' approach is one in which the data item is required to be stored. That approach is essentially the antithesis of

Appellant's approach, as will now be discussed in detail.

A core feature of Appellant's invention is that the **data item** of interest (e.g., sensitive information) **is itself <u>never</u> stored**. How can this be? The data item of interest is something that the user already has memorized, such as the user's Social Security number or a password, or has alternative access to, such as the user's credit card number. Thus, to make sure that Appellant's own lockbox system cannot possibly be a source of data leak (e.g., for identity theft), Appellant's claimed approach is to discard (i.e., not store) the data item to be protected. Consider the following from Appellant's Background Section (describing the problems of the prior art):

> Another solution that solves much of this growing problem involves running a software agent to monitor the PC's network traffic. This simplified or basic "lockbox" approach ensures that sensitive information is not transmitted outside the local host without the user's knowledge. If sensitive information is discovered during this process, the underlying security engine may give the user the ability to block or modify the outgoing request. [...]
>
> The simplified lockbox approach has its problems, however. **Storage of reference copies of the sensitive information in a simple lockbox creates a new point of vulnerability. The lockbox itself becomes a potential target for attack and compromise.** Therefore, a better solution is sought.

(Appellant's Specification, at [0011] - [0012]; Emphasis added)

Importantly, in order to avoid the above-identified vulnerability (as described in Appellant's Background Section), the data item itself is not stored at all in Appellant's system -- and that fact is explicitly set forth in Appellant's claim limitations.

Given that the data item is not stored in Appellant's system, how is it possible for Appellant's system to protect that data item (e.g., from outbound transmission of user input on a form)? The data item of interest to Appellant's invention typically comprises

"input of sensitive information from a user" (see, e.g., Appellant's claim 1), such as a Social Security number, a password, or the like. As noted above, this sensitive information is not stored since, if it were stored, then it may serve as a point of vulnerability (i.e., subject to attack and compromise by hackers, etc.). Instead, a data "shadow" is created so that the original input of the sensitive information may in fact be purposely discarded. Therefore, not only is the sensitive information not stored in Appellant's system, but also the data shadow is created for the express purpose of allowing the original data item (input of sensitive information) to be discarded. By discarding the data item (e.g., Social Security number, password, etc.), that data item no longer remains as vulnerable data present on the user's system. No matter how hard a hacker tries, he or she will be unable to retrieve a copy of the sensitive information from Appellant's lockbox on the user's system, as no copy in fact exists in the lockbox itself. Further, the hacker will be unable to reconstitute the sensitive information from the data shadow, as the data shadow itself is a cryptographically secured hash (e.g., MD-5), which makes reconstitution of the original sensitive information computationally infeasible.

Although Appellant's originally filed claims were believed to distinguish over the cited art, the claims were nevertheless amended in Appellant's last-filed Amendment to further clarify Appellant's claimed invention and expedite prosecution of the present application. For example, independent claim 1 was amended to include the claim limitation of (shown in amended form):

> computing a data shadow of the sensitive information for storage in a repository, and thereafter discarding the input so that the sensitive information itself is not stored;

(Appellant's other independent claims were amended in a like manner.) The foregoing amendment to the claim makes it explicitly clear that the sensitive information itself is in fact discarded after computation of the data shadow. The sensitive information itself is **not stored** at all, as part of the process. In fact, if the sensitive information were stored, that would defeat the purpose of Appellant's invention. The primary purpose and utility of Appellant's invention is an improved lockbox that stores data "shadows," so that the

underlying sensitive information itself **never need be stored** on the subject computer (in contrast to prior art approaches). In this manner, Appellant's system can employ the data shadows to detect any attempted transmissions of sensitive information (e.g., from future keyboard input by the user), even though a copy of the sensitive information itself is not and was not ever stored on the subject computer.

In response to Appellant's last-filed Amendment, the Examiner states: "**Margolus et al. teaches that a data-item is deposited** if a data-name, which is a digitally fingerprinted data-item, is not already in the data repository. Margolus et al. teaches that digitally fingerprinted data-item is stored in the repository and not the actual data-item." (Emphasis added.) As shown, the Examiner acknowledges that Margolus teaches an approach where the data item of interest is in fact stored or deposited by that system -- directly in contrast to Appellant's approach. (To the extent that the second half of the Examiner's statement appears to contend that the data item itself is not stored in the Margolus data repository that contention is incorrect, as shown below.) In Appellant's system (and as required by Appellant's claims), the data item is never stored and is actively discarded or purged from the system upon computation of the data shadow. And in fact, the above-described approach of Margolus to store a copy of the data item would, if incorporated into Appellant's system, destroy a key advantage of Appellant's system -- that is, that it does not ever store a copy of the data item and therefore does not become a point of vulnerability.

Margolus' system is a network storage solution that employs digital fingerprints to avoid unnecessary duplicate transmission or storage of a given data item. The Examiner has attempted to "shoehorn" Margolus' approach into Appellant's security system and method claims, but Margolus simply does not fit. Margolus provides no teaching or suggestion that would suggest his system may detect and trap outbound transmission of sensitive user information, all without ever storing a copy of the user information itself.

Moreover, Margolus describes his system and data repository in sufficient detail that it is easy to discern that Margolus' system cannot function in a manner required by Appellant's claims (and contended by the Examiner). For example, at the outset (i.e., first sentence of Margolus Summary), Margolus states:

> [0010] In general, the invention features a method by which more than one client program connected to a network **stores the same data item on a storage device of a data repository** connected to the network. The method comprises encrypting the data item using a key derived from the content of the data item, determining a digital fingerprint of the data item, **and storing the data item on the storage device** at a location or locations associated with the digital fingerprint.
> (Emphasis added.)

From the foregoing passage, it is clear that Margolus describes a data item storage/retrieval mechanism, which of course has as its primary purpose the task of in fact storing the data item. This is of course necessary since at some point, the user of Margolus' system will retrieve the data item for use. The Examiner's contention that Margolus' avoidance of redundantly storing a data item (i.e., avoiding storing multiple identical copies) is the same as Appellant's never storing a copy (and actively discarding or purging the input) is a non sequitur. Clearly, Margolus' system stores a copy of the data item of interest and any software lockbox system constructed based on that approach would fare no better than the prior art simplified lockbox systems described in Appellant's Background Section. Specifically, it would pose a point of vulnerability since it in fact does store a copy of the data item that hackers may attack.

Margolus' description of how his data repository is constructed further highlights these distinctions. Margolus states:

> [0058] The data repository is a distributed aggregate of data storage devices connected to the network, which together maintain a collection of data-items in a single logical address space, indexed by "datanames" (digital fingerprints) generated directly from the data-items themselves. Logically only one copy of each distinct data-item is kept in the repository, which allows for great economy in use of storage space. In practice, some redundancy is needed in order to assure data integrity, and to increase data availability and accessibility.

As set forth above, Margolus' system is in fact a storage system, and thus has as its primary purpose the storage of data items. The improvement noted by Margolus is use of digital fingerprints to facilitate the storage and transmission of data items (i.e., mainly, to avoid duplicate storage and duplicate/unnecessary transmissions). If one were to design a software lockbox security system based on Margolus' storage approach (i.e., maintaining a reference copy of the data item of interest), one would be left with a system that fared no better than a simplified lockbox. Importantly, all those systems have a particular problem that makes them acceptable: **Storage of reference copies of the sensitive information in a simple lockbox [or Margolus's network data repository] creates a new point of vulnerability. The lockbox itself becomes a potential target for attack and compromise.** Therefore, a better solution was sought and was the impetus for Appellant's improved lockbox invention.

All told, Appellant's improved lockbox approach (which expressly eschews storage of the data item itself) is not taught or suggested by Margolus' network storage solution, which clearly stores at least one copy of the data item of interest, as it is in fact a network storage system. As Margolus' approach is in fact one "promoting" the storage of a data item itself on network storage, the Margolus' approach would at best teach a system that poses the same exact point of vulnerability present in prior art lockbox approaches. Margolus teaches, if anything in this regard, away from Appellant's claimed approach. It is respectfully submitted that the claims set forth a patentable advance over the art, and that any rejection under Section 102(e) should not be sustained.

B. Conclusion

The present invention greatly improves the ease and efficiency of the task of preventing unauthorized transmission of sensitive user information, such as malware (malicious software) transmission of Social Security numbers, credit card numbers, passwords, and the like. It is respectfully submitted that the present invention, as set forth in the pending claims, sets forth a patentable advance over the art.

In view of the above, it is respectfully submitted that the Examiner's rejections under 35 U.S.C. Section 102 should not be sustained. If needed, Appellant's undersigned

attorney can be reached at 408 884 1507. For the fee due for this Appeal Brief, please refer to the attached Fee Transmittal Sheet. This Brief is submitted electronically.

Respectfully submitted,

Date: November 13, 2007

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX

8. CLAIMS APPENDIX

1. In a computer system, a method for protecting sensitive information, the method comprising:

receiving input of sensitive information from a user;

computing a data shadow of the sensitive information for storage in a repository, and thereafter discarding the input so that the sensitive information itself is not stored;

based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and

blocking any detected attempt to transmit the sensitive information that is not authorized by the user.

2. The method of claim 1, wherein said sensitive information comprises structured data.

3. The method of claim 2, wherein said data shadow is computed for the structured data as a regular expression and a hash.

4. The method of claim 3, wherein said hash comprises a MD-5 hash.

5. The method of claim 2, wherein said structured data includes credit card number information.

6. The method of claim 2, wherein said structured data includes Social Security number information.

7. The method of claim 3, wherein said regular expression represents formatting information for said structured data.

8. The method of claim 3, wherein said hash is computed after normalization of the structured data.

9. The method of claim 8, wherein said normalization includes removing any formatting information before computing the hash.

10. The method of claim 1, wherein said sensitive information comprises structured data and said detecting step includes:

initially detecting said structured data by matching a format for that structured data.

11. The method of claim 1, wherein said sensitive information comprises literal data.

12. The method of claim 11, wherein said data shadow is computed for the literal data as a length value plus at least one hash of the literal data.

13. The method of claim 12, wherein said at least one hash includes an additional first pass hash or checksum value computed for the literal data.

14. The method of claim 12, wherein said at least one hash includes a MD-5 hash computed for the literal data.

15. The method of claim 1, wherein said at least one hash includes an optional checksum value computed for the literal data that allows relatively quick detection of the sensitive information and a MD-5 hash that allows subsequent verification.

16. The method of claim 1, wherein said receiving input step includes:

receiving input indicating a type for the sensitive information.

17. The method of claim 16, wherein said receiving input indicating a type includes:

receiving input indicating that the sensitive information is a password.

18. The method of claim 16, wherein said receiving input indicating a type includes:

receiving input indicating that the sensitive information is a Social Security number.

19. The method of claim 16, wherein said receiving input indicating a type includes:

receiving input indicating that the sensitive information is a credit card number.

20. The method of claim 16, wherein said receiving input indicating a type includes:

receiving input indicating that the sensitive information is a personal identification number (PIN).

21. The method of claim 1, further comprising:

automatically determining a type for the sensitive information that indicates formatting.

22. The method of claim 21, wherein said step of automatically determining a type includes:

matching the input against a template for identifying a type.

23. The method of claim 1, wherein said detecting step includes:

trapping an outbound buffer of data that may contain the sensitive information; and

in instances where the sensitive information comprises structured data, performing a regular expression search on the outbound buffer.

24. The method of claim 23, further comprising:

if a regular expression match is found, normalizing data from the match so as to remove formatting and thereafter computing a hash on it, for comparison with

corresponding hash values stored in the repository.

25. The method of claim 24, wherein said hash is a MD-5 hash.

26. The method of claim 1, wherein said detecting step includes:

trapping an outbound buffer of data that may contain the sensitive information; and

in instances where the sensitive information comprises literal data, performing a sliding window search on the outbound buffer.

27. The method of claim 26, wherein said sliding window search includes performing an optional checksum calculation on successive blocks of bytes within the outbound buffer, for comparison with corresponding checksum values stored in the repository.

28. The method of claim 27, further comprising:

if a match is found based on the checksum comparison, verifying the match with a MD-5 hash performed on data from the match.

29. The method of claim 28, wherein said MD-5 hash performed on data from the match is compared against a corresponding MD-5 hash value stored in the repository.

30. The method of claim 1, wherein said step of blocking includes:

referencing a stored policy indicating whether the sensitive information should be blocked from transmission.

31. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

32. A downloadable set of processor-executable instructions for performing the method of claim 1.

33. In a computer system, a method for securing sensitive items from inappropriate access, the method comprising:

receiving input from a user indicating that a particular sensitive item is to be protected from inappropriate access;

storing metadata characterizing the particular sensitive item, and thereafter discarding the input so that the particular sensitive item itself is not stored;

based on the stored metadata, detecting whether the particular sensitive item is present in any transmission of outgoing data; and

trapping any transmission of outgoing data that is detected to contain the particular sensitive item.

34. The method of claim 33, further comprising:

a policy indicating what action the system should be taken upon trapping transmission of outgoing data that contains the particular sensitive item.

35. The method of claim 34, wherein said action includes blocking any trapped transmission.

36. The method of claim 34, wherein said action includes querying the user about whether the particular sensitive item may be transmitted.

37. The method of claim 33, wherein said metadata includes a one-way hash of the particular sensitive item.

38. The method of claim 37, wherein said one-way hash comprises a MD-5 hash.

39. The method of claim 33, wherein said particular sensitive item comprises structured data, and wherein said metadata includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data.

40. The method of claim 39, wherein said trapping step includes:

locating the particular sensitive item by first performing a regular expression search on the outgoing data for finding a match based on formatting; and

for any match found based on formatting, performing a hash on the match to determine whether it matches a corresponding hash stored as part of the metadata.

41. The method of claim 33, wherein said particular sensitive item comprises literal data and wherein said metadata comprises as a length value plus at least one hash of the literal data.

42. The method of claim 41, wherein said trapping step includes:

locating the particular sensitive item by first performing a sliding window search through the outgoing data for a block of bytes having a size equal to said length value and having a hash value equal to one of said at least one hash of the literal data.

43. The method of claim 42, wherein said at least one hash includes a MD-5 message digest computation.

44. The method of claim 43, wherein said at least one hash further includes an optional first pass hash or checksum as an optimization.

45. A computer-readable medium having processor-executable instructions for performing the method of claim 33.

46. A downloadable set of processor-executable instructions for performing the method of claim 33.

47. A system providing security for sensitive information, the system comprising:

a data processing system receiving input of sensitive information;

a secure lockbox module for storing a secure descriptor characterizing the

sensitive information, so that the system can detect transmission of the sensitive information without a copy of the sensitive information itself being stored; and

a security module for detecting, based on said secure descriptor, any attempted transmission of outgoing data that contains the sensitive information.

48. The system of claim 47, wherein said input includes an indication of a type for the sensitive information.

49. The system of claim 48, wherein said indication of a type includes a selected one of structured data and literal data.

50. The system of claim 49, wherein said structured data includes a credit card number.

51. The system of claim 47, further comprising:

a security policy specifying what action is to be undertaken when the security module detects an attempt to transmit the sensitive information.

52. The system of claim 51, wherein said security policy specifies an action of blocking any attempted transmission of the sensitive information.

53. The system of claim 51, wherein said security policy specifies an action of prompting a user to allow or deny any attempted transmission of the sensitive information.

54. The system of claim 47, wherein said sensitive information includes structured data, and wherein said secure descriptor includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data.

55. The system of claim 47, wherein said sensitive information includes literal

data and wherein said secure descriptor includes a length value plus at least one hash of the literal data.

9. EVIDENCE APPENDIX

This Appeal Brief is not accompanied by an evidence submission under §§ 1.130, 1.131, or 1.132.

10. RELATED PROCEEDINGS APPENDIX

Pursuant to Appellant's statement under Section 2, this Appeal Brief is not accompanied by any copies of decisions.